Status of the Claims

Claims 1-29. (Cancelled)

5   30. (Currently Amended) A process, comprising the steps of:

purchasing usage rights for an encrypted asset by sending purchase information for an asset from a client machine to a store server;

sending a ticket from the store server to the client machine, the ticket comprising an asset ID corresponding to the purchased encrypted asset;

10   sending an asset request a request for the purchased encrypted asset using the asset ID from the client machine to the a fulfillment server;

sending the purchased encrypted asset from the fulfillment server to the client machine in response to the received asset ID;

sending a license request from the client machine to the fulfillment server;

15   sending a license from the fulfillment server to the client machine, the license comprising an asset key and the usage rights associated with the purchased encrypted asset;

encrypting the asset key and the usage rights at the client machine;

binding the encrypted asset key to the client machine;

20   combining the machine-bound encrypted asset key and encrypted user rights into machine-bound asset rights;

storing the machine-bound asset rights within a secure key locker within the client machine;

sending an acknowledgement of the receipt of the purchased encrypted

25   asset and the license from the client machine to the fulfillment server;

receiving a user request at an output module within the client machine, the user request received from a user for use of the encrypted asset;

sending an asset rights request from the output module through a tamper resistant asset rights module within the client machine to the secure key locker to

30   get the machine-bound asset rights;

receiving the machine-bound asset rights at the tamper resistant asset rights module from the secure key locker in response to the asset rights request;

breaking the machine-bound asset rights at the tamper resistant asset rights module into the encrypted asset key and the encrypted usage rights;

sending the encrypted asset key and the encrypted usage rights from the tamper resistant asset rights module to the output module;

decrypting the machine-bound encrypted usage rights at the output module;

5   determining at the output module if the use of the encrypted asset requested by the user is allowed by the machine-bound usage rights;

conditionally

decrypting the encrypted asset key,

decrypting the encrypted asset with the decrypted asset key, and

10   serving the user request,

if the use of the encrypted asset requested by the user is determined to be allowed by the machine-bound usage rights; and

~~controlling usage of the purchased asset within the client machine based on the received license; and~~

15   updating the machine-bound usage rights within the secure key locker within the client machine if the machine-bound usage rights are affected by the use~~, in accordance to the controlled usage~~.

31.   (Currently Amended) The process of Claim 30, further comprising the steps

20   of:

saving the ~~purchased~~ encrypted asset to an asset store at the client machine; and

attaching machine characteristics to the license~~; and~~

~~securely storing the license at the client machine~~.

25

32.   (Previously Presented) The process of Claim 31, wherein the machine characteristics comprise a unique identifier associated with the client machine.

33.   (Previously Presented) The process of Claim 31, wherein the machine

30   characteristics comprise a unique machine fingerprint associated with the client machine.

34.   (Currently Amended) The process of Claim 31, further comprising the step of:

35   launching a digital content player to play the ~~purchased~~ encrypted asset at the client machine.

35. (Currently Amended) The process of Claim 34, wherein the digital content player allows usage of the purchased <u>encrypted</u> asset on the client machine if the asset key and the <u>machine-bound</u> usage rights associated with the
5   purchased <u>encrypted</u> asset are present at the client machine.

36. (Currently Amended) The process of Claim 35, wherein the allowed usage of the purchased <u>encrypted</u> asset is determined by the <u>machine-bound</u> usage rights associated with the purchased <u>encrypted</u> asset.
10

37. (Currently Amended) The process of Claim 34, wherein the digital content player prevents usage of the purchased <u>encrypted</u> asset on the client machine if the if the asset key and <u>machine-bound</u> usage rights associated with the purchased <u>encrypted</u> asset are absent from the client machine.
15

38. (Currently Amended) The process of Claim 30, wherein the purchased <u>encrypted</u> asset comprises any of a song, an album, a video, a movie, and a video game.

20   39. (Withdrawn) A digital content store system established across a network to a plurality of client machines, comprising:
        a plurality of encrypted assets located at a server connected to the network;
        a plurality of access keys uniquely associated with each of the encrypted
25   assets;
        available usage rights associated with each of the encrypted assets;
        means for selectable purchase for at least one encrypted asset at the client machines, wherein upon a purchase transaction between a client machine and the server, the purchased asset, the asset key associated with
30   purchased asset, and the corresponding usage rights are sent to the client machine;
        means for binding the sent usage rights to the receiving client machine, wherein the encrypted asset is enabled by the asset key to be used at the client machine only if the machine-bound usage rights are present at the client
35   machine;

means for controlling usage of the purchased asset within the client machine; and

means for updating the machine-bound usage rights within the client machine, in accordance with the controlled usage.

5

40. (Withdrawn) The system of Claim 39, wherein the usage comprises playing the enabled purchased asset.

41. (Withdrawn) The system of Claim 39, wherein the usage rights are updated
10   based upon a playing of the enabled purchased asset.

42. (Withdrawn) The system of Claim 39, wherein the usage comprises burning the enabled purchased asset to a medium.

15   43. (Withdrawn) The system of Claim 42, wherein the usage rights are updated based upon a burning of the enabled purchased asset.

44. (Withdrawn) The system of Claim 39, wherein the usage comprises loading the enabled purchased asset to a digital content player.

20

45. (Withdrawn) The system of Claim 40, wherein the usage rights are updated based upon a loading of the enabled purchased asset to the digital content player.

25   46. (Withdrawn) The system of Claim 39, wherein the encrypted purchased asset comprises any of a song, a playlist, a movie, and a video game.

47. (Withdrawn) A controllable asset system between a client machine and a content store across a network, comprising:

30   an encrypted asset located at the client machine;

an asset key located at the client machine, the asset key associated with the encrypted asset;

usage rights located at the client machine, the usage rights associated with allowed use of the encrypted asset;

35   a license bound to the client machine and associated with the usage rights;

means for internally managing usage of the encrypted asset within the client machine, wherein the asset key is conditionally usable to decrypt the encrypted asset only if the machine bound license is present at the machine, and if the use is allowed by the usage rights; and

5   means for updating the machine-bound usage rights within the client machine, in accordance to the internally managed usage.

48. (Withdrawn) The system of Claim 18, wherein the usage rights comprise a burn count.

10

49. (Withdrawn) The system of Claim 19, wherein further use of the encrypted asset at the client machine is allowed only if the current burn count is confirmed to be acceptable at the content store.

15   50. (Withdrawn) The system of Claim 19, wherein further use of the encrypted asset at the client machine is allowed only if the current burn count is confirmed to be acceptable at the client machine.

51. (Withdrawn) A process, comprising the steps of:

20   receiving at least one digital asset;

encoding each of the received digital assets;

encrypting the encoded digital assets;

generating an asset key associated with the encrypted encoded digital assets;

25   establishing usage rights for the encrypted digital assets;

authorizing the usage rights of at least one of the encrypted digital assets for a user at a client machine;

sending the authorized encrypted digital asset, the asset key, and the usage rights to the authorized client machine;

30   binding the usage rights to the authorized client machine;

securely storing the usage rights at the authorized client machine;

providing authorized usage of the encrypted digital asset with the asset key within the client machine; and

if usage rights are affected by the authorized usage, updating the usage

35   rights within the client machine.

52. (Withdrawn) The process of Claim 51, wherein the digital assets comprise any of a song, a playlist, a movie, and a video game.

53. (Withdrawn) The process of Claim 51, wherein the authorized usage rights comprise play of at least one of the encrypted digital assets on the authorized client machine.

54. (Withdrawn) The system of Claim 53, wherein the authorized usage rights are updated within the client machine based upon a playing of at least one of the encrypted digital assets.

55. (Withdrawn) The system of Claim 51, wherein the authorized usage comprises burning at least one of the encrypted digital assets to a medium.

56. (Withdrawn) The system of Claim 55, wherein the authorized usage rights are updated within the client machine based upon the burning of at least one of the encrypted digital assets.

57. (Withdrawn) The system of Claim 51, wherein the authorized usage comprises loading the encrypted digital asset to a digital content player.

58. (Withdrawn) The system of Claim 58, wherein the authorized usage rights are updated within the client machine based upon a loading of at least one of the encrypted digital assets.

59. (New) The process of Claim 38, further comprising the step of:
        playing a sample of the asset if the digital content player detects any that the key is missing or is not valid for the client machine.

60. (New) The process of Claim 59, further comprising the step of:
        presenting the user with a purchase opportunity.

61. (New) The process of Claim 60, further comprising the step of:
        transferring the user to the digital music store to complete the process if the user chooses to purchase based upon the presented purchase opportunity.

62. (New) The process of Claim 30, wherein the use of the encrypted asset comprises playing the asset.

63. (New) The process of Claim 30, wherein the use of the encrypted asset comprises burning the asset to a medium.

64. (New) The process of Claim 30, wherein the use of the encrypted asset comprises loading the asset to a digital content player.

65. (New) The process of Claim 30, further comprising the step of:

launching a download manager at the client machine with the received ticket;

wherein the asset request is sent from the launched download manager at the client machine to the fulfillment server.